An Extensive Survey of Color Image Watermarking Based on Transforms

Sandeep Kumar, Prof. Anshul Sarawagi[2], Prof. Aishwarya Mishra[3]

[1]M-Tech Research Scholar, [2]Research Guide, [3]HOD

Department of Computer Science Engineering, IES College, Bhopal

Abstract - In the recent years, a huge amount of digital information is circuiting through all over the world by means of the World-Wide Web. Most of this data is exposed and can be easily forged or corrupted. The need for intellectual property rights protection arises. Digital watermarking has been proposed as one of the possible ways to deal with this problem, to keep information safe. The watermarking of digital data has become very popular approach for intellectual property rights protection. Several watermarking techniques were developed and a large amount of methods were proposed, but still the most of known ways to protect data are far from ideal. The digital data of the various types such as text, images, audio, video can be processed by the watermarking procedure. In general, all types of data watermarking techniques have similar simple ideas - to hide a set of owner's data within the materials, which should published, with the purpose to be able to prove his ownership. The security of the watermark image using encryption technique. the three domains or techniques the DWT, DCT and SVD for watermarking. the embedding and extraction algorithms based on DWT-DCT-SVD for grayscale image and color image. The existence of these watermarks with in a multimedia signal goes unnoticed except when passed through an appropriate detector. Common types of signals to watermark are still images, audio, and digital video.

Keyword- Digital Image Watermarking, DWT, Chirp z-transform (CZT), Entropy, SVD, QR.

I. INTRODUCTION

Digital watermarking is one of the most influential techniques to detect misappropriated data and ensure copyright protection for the digital content like texts, images, audios and videos from illegal manipulations. Digital watermarking refers to the process of embedding or hiding the digital data directly onto the digital content (multimedia) and that it can be extracted again. And It has many proprieties such as cryptography, watermark is imperceptible and does not affect the aesthetic of the digital content and robustness of the watermark against different attacks such as the compression, rotation and scaling for digital image watermarking.

The digital multimedia like the image, video and audio, can be protected against copyright infringements using some techniques such as steganography and digital watermarking techniques. Digital Watermarking is a technique to insertion of data into digital multimedia, without affecting quality of the original multimedia. Therefore, this technique has become useful tool for steganography, copyright protection and content authentication. Where, the digital watermarking technology plays an important role in preventing copyright violation as it allows to place an imperceptible or invisible watermark depending on the requirement in the multimedia data to detect malicious tampering of the multimedia or data identify the legitimate owner.

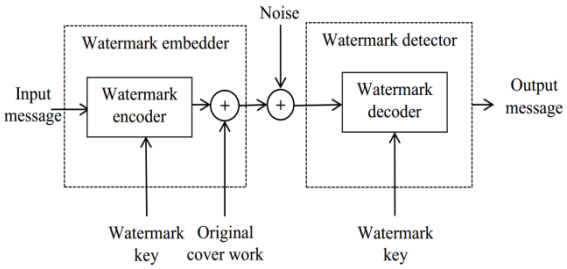

Figure 1.1 standard model for watermarking.

Discrete Wavelet Transformation (DWT)

DWT is used to decompose the input image into sub bands of different resolutions that are low, middle and high frequency bands. The mean value of the filter is the low frequency coefficient while wavelet coefficients are the high frequency coefficients [10].In one level DWT, an image is decomposed into four sub-bands which are approximate sub-band (LL1), horizontal sub-band (HL1), vertical sub-band (LH1), and diagonal Sub-band (HH1) [11][12]. One level DWT of an image as shown in following fig.

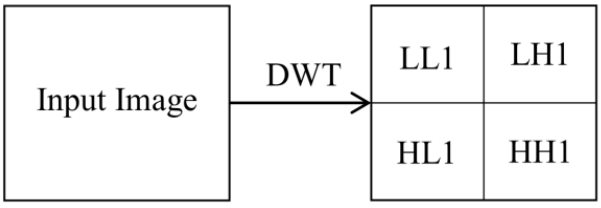

Fig. Decomposition structure "one level DWT".

Digital image watermarking applications

- Fingerprinting:

A watermark can be used to trace the source of breach of the copyright agreement. Different watermarking keys are embedded into the copies provided to different customers. A unique watermark guarantees the possibility of finding the customer providing the copies of the product illegally to a third party.

- Indexing:

Watermarking is widely applied in a number of multimedia applications not only for the purpose of protection of the information but also to insert some kind of indexing or comments into video or other multimedia content. As the use of the Internet and in particular search engines increases indexing would simplify access to the data, and watermarking is useful in this respect.

- Copyright Protection & Owner identification:

This application is connected with Fingerprinting, but this is a more generalized area. Watermarking primary use is protection of data copyright information. A watermark representing the information about the owner is inserted into the data to be able to prove the ownership right.

- Broadcast monitoring:

Watermarking can be used to help automate the identification of broadcast programs. A watermark is inserted into the data broadcasted over the network, be it radio or TV. It assures that advertisers receive the airtime they have paid for or the property rights for music or video data.

II. Digital image watermarking approaches

The scheme of digital image watermarking divides into two stages: the embedding process and the detection process as shown in following figures. The embedding process is used for embedding the watermark image into the cover image with the secret key to secure the watermark image. The output of this process is the watermarked image. And, the detection process is used to recover the watermark by using the same secret key.

- Embedding watermarking

As it was mentioned above, we did the PCA transform first, after that we embedded watermark and compared qualities of the images after reconstruction. For the quality measurement we used the Peak-Signal-to-Noise Ratio, which can be calculated in the following way,

$$PSNR = 10 \log 0$$

where EWM is the energy of difference between the original image and the watermarked one. Parameters x and y are spatial sizes of the image, m is a spectral size, s is the peak value of the original image.

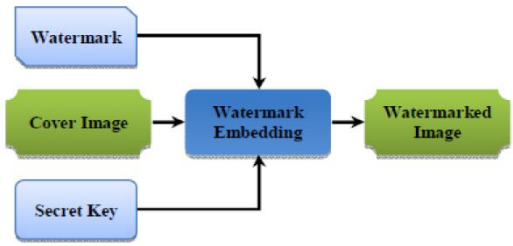

Fig.2.1 the embedding process.

- Detection watermarking

The whole procedure looks pretty similar to the watermark extraction one, but the initial data, which we know, differs. In the case of the watermark extraction - we have the original image and an entire embedding knowledge such as input parameters and obtained by means of the PCA transform eigenvectors database or just eigenvectors database. In case of the detection we have almost nothing - no knowledge about the embedding method or any useful data except original image. Data set for this approach is the original image and watermarked one. Using as a base these facts we can try to detect whether watermark is emedded or not. The main advantage of this approach is following - we don't have to know the method of the watermark embedding. The ICA algorithm is applied to all bands of these images, and by result images we obtained we make a conclusion.

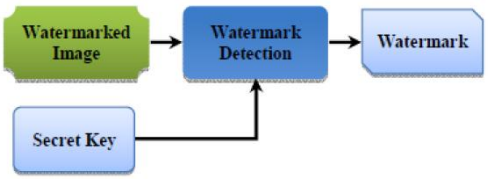

Fig.2.2 the detection process.

- Extraction watermarking

First algorithm is based on a backward embedding formula defined in Eq.

$$watermark = \frac{(band_{wm}(n) - \alpha_1 band(m))}{\alpha_2}$$

where a1s a2 are strength coefficients used for embedding, the band(m) is a mth component of PCA-transformed spectral domain of the original image and bandwm(n) is the nth one of the PCA-transform result applied to watermarked image. The PCA transform uses eigenvectors kept by owner. So, it is assumed that owner of the original image has all information, needed for watermark extraction.

Singular Value Decomposition (SVD)

$$A(M * N) = U(M * M)S(M * N)V(N * N)$$

The SVD is one of linear algebra tools. And, it is an approximation and factorization technique that effectively reduces any matrix into a smaller invertible matrix, where SVD of a rectangular matrix A is a decomposition of the form,

Where U and V are orthogonal matrices and S (sigma) is a diagonal matrix. The columns of U are called the left singular vectors and the columns of V are called the right singular vectors and the diagonal elements of S are called the singular values (non-negative diagonal elements in decreasing order).

III. LITERATURE SURVEY

S. No.	Title	Author	Year	Approach
1	Colour image watermarking based on wavelet and QR decomposition,	P. Rasti, G. Anbarjafari and H. Demirel	2017	a new image watermarking algorithm on colour images is proposed. The proposed algorithm divides a cover image into three colour bands of red, green and blue.
2	A transform domain based robust color image watermarking scheme for single and dual attacks,	N. N. Hurrah, N. A. Loan, S. A. Parah and J. A. Sheikh	2017	an efficient watermarking scheme based on hybrid transform domain. The watermarking scheme is blind, robust and secure.
3	Novel blind colour image watermarking technique using Hessenberg decomposition	Q. Su	2016	a novel blind image watermarking technique using Hessenberg decomposition is proposed to embed colour watermark image into colour host image.
4	ROI lossless colored medical image watermarking scheme with secure embedding of patient data,	S. Deepa and A. Sandeep,	2016	This paper focuses on reversible watermarking of medical images, both grey scale as well as color, preserving its ROI.
5	A New Colour Image Watermarking Technique Using Special Domain	A. M. A. Najih, S. A. R. Al-Haddad, A. R. Ramli and S. J. Hashim	2015	a robust colour image watermarking algorithm utilizing a block probability in a spatial domain is recommended by this study
6	Color image watermarking using wavelet packet transform	R. Mothi and M. Karthikeyan	2014	an effective watermarking technique based on a Wavelet Packet Transform (WPT).
7	A colour image watermarking technique resistant to affine geometric attacks	F. O. Owalla and E. Mwangi	2013	This paper presents a colour image watermarking scheme resistant to affine geometric distortions.
8	A new colour image watermarking scheme using Cellular Automata Transform and Schur decomposition	N. Panahi, M. Amirani, S. Behnia and P. Ayubi	2013	a novel robust colour image watermarking scheme in Cellular Automata Transform (CAT) domain in combination with Schur decomposition is presented.

P. Rasti, G. Anbarjafari and H. Demirel[1] In this work, a new image watermarking algorithm on colour images is proposed. The proposed algorithm divides a cover image into three colour bands of red, green and blue. Then the following tasks are done on all three channels separately. First, Each colour band is divided into patches of small sizes then the entropy of each patch is calculated. At this step a threshold is found based on the average entropy of all patches and following is applied to all patches which have entropy lower than the threshold. A wavelet representation of each patch are given by applying a discrete wavelet transform. Then Singular value decomposition, orthogonal-triangular decomposition, and a chirp z-transform are used to embed a watermark on the cover image. Several signal processing attacks are applied on watermarked images in order to robustness of the algorithm.The Proposed algorithm is compared with one conventional and two state-of-the-art algorithms. Experimental results show superiority of the proposed algorithm compare with other algorithm in the area of image watermarking.

N. N. Hurrah, N. A. Loan, S. A. Parah and J. A. Sheikh[2] This paper proposes an efficient watermarking scheme based on hybrid transform domain. The watermarking scheme is blind, robust and secure. The scheme has been developed to withstand dual attacks which may be combination of signal processing and geometric attacks. For achieving the said goals, a single watermark has been embedded in all the three components (RGB) of the color image using a new interblock differencing method in discrete cosine transform (DCT) domain. Discrete wavelet

transform (DWT) is used prior to embedding in order to get LL sub-band from each of the three color image components. The principle of maximum probability is applied to select the watermark bit after extracting the watermark from the three components of the color image. Multiple encryption techniques have also been employed in order to increase the security of the watermark. The experimental results prove that the proposed scheme is highly robust to almost all kind of signal processing attacks including geometric attacks like rotation, cropping and resizing. Also the watermarked image is subjected to two simultaneous attacks one after other to prove the robustness of the scheme to dual attacks. The results hence obtained for different attacks are presented in terms of parameters like PSNR, NCC, BER and BCE to test the performance of the scheme.

Q. Su,[3] In this study, a novel blind image watermarking technique using Hessenberg decomposition is proposed to embed colour watermark image into colour host image. In the process of embedding watermark, the watermark information of colour image is embedded into the second row of the second column element and the third row of the second column element in the orthogonal matrix obtained by Hessenberg decomposition. In the process of extracting watermark, neither the original host image nor the original watermark image is needed and it is impossible to retrieve them without the authorised keys. Experimental results show that the proposed colour image watermarking technique based on Hessenberg decomposition outperforms other watermarking methods and it is robust to resist a wide range of attacks, e.g. image compression, filtering, cropping, rotation, adding noise, blurring, scaling, sharpening and rotation and so on. Especially, the proposed method has lower computational complexity than other methods based on singular value decomposition or QR decomposition.

S. Deepa and A. Sandeep,[4] Transmission of images via internet and it's authentication is of great importance with the booming techniques in the field of networking and information security. Medical imaging and it's secure transmission have grown up as a necessity. This paper focuses on reversible watermarking of medical images, both grey scale as well as color, preserving its ROI. It also effectively manages patient health record by securely embedding it inside the image before transmission which facilitates better archiving of data with comparatively lesser transmission bandwidth and much lesser chaos. This paper considers noisy and noiseless environments as different cases with different implementation for both. Also tamper detection and recovery of ROI makes this quite a useful technique in the upcoming color imaging era.

A. M. A. Najih, S. A. R. Al-Haddad, A. R. Ramli and S. J. Hashim[5] Safeguarding the due rights of multimedia property ownership has recently emerged as a significant challenge to players in this sphere. In response to this issue, a robust colour image watermarking algorithm utilizing a block probability in a spatial domain is recommended by this study. The protection of the watermark is fortified through the employment of the Arnold transform to scramble watermark pixels. Decomposition of the cover image into Red, Green, and Blue channels is executed and the green channel is favoured for the embedding procedure. The reorganization of the scrambled watermark is achieved with the utilization of sequence numbers generated by a secret key. Four embedding's of the encoded watermark are carried out at separate points in the green channel of the colour image. The embedding of all the bits of the binary encrypted watermark is realized by regulating the strengths of a non-overlapping 8×8 sized component of the cover image green channel. The watermark extraction procedure involves a comparison between the strengths of an 8×8 sized component of the initial and watermarked images as well as calculations to uncover the likelihood of recognizing (0 or 1). The algorithm design was deemed invulnerable and exhibited robustness when confronted with a substantial number of image processing onslaughts.

R. Mothi and M. Karthikeyan,[6], The paper proposes a new image watermarking technique for digital media that can embed a specified watermark image in the cover image without affecting the imperceptibility and increase the security of watermarks. Watermarking techniques based on DCT (Discrete Cosine Transform) and Wavelet Transform are studied, whereas by using wavelet packet transform the robustness of the technique can be achieved compared to other transforms. This paper urges an effective watermarking technique based on a Wavelet Packet Transform (WPT). Here the image has been divided into several bands using wavelet packet and in particular subband the watermark is embedded. The sub band selection is achieved by calculating the energy value for each band and suitable band is selected for embedding the watermark into the cover image. The extraction of watermark is carried out by taking the inverse transform to the watermarked image and with the help of cover image the watermark has been extracted. The Peak Signal to Noise Ratio (PSNR) value has been calculated to analyze the quality of image.

F. O. Owalla and E. Mwangi,[7] This paper presents a colour image watermarking scheme resistant to affine geometric distortions. The technique involves embedding of the watermark in the host image in the Discrete Cosine Transform (DCT) domain in a spread-spectrum format. Harris corner detector based feature-points are then

employed to get Delaunay triangulation which is used to reverse geometric attacks before attempting to extract the watermark. In some instances the geometric attack may lead to loss of feature-points resulting in the recovery of low quality watermark. In this paper we propose a scheme of estimating geometric attacks by taking the mean of selected triangles in the Delaunay tessellation. Computer simulation using MATLAB has been used to show the robustness of the proposed scheme.

N. Panahi, M. Amirani, S. Behnia and P. Ayubi[8] In this work a novel robust colour image watermarking scheme in Cellular Automata Transform (CAT) domain in combination with Schur decomposition is presented. Via different CA bases functions, the CAT domain provides numerous transform patterns, hence it improves the flexibility and security in data hiding. Furthermore, through Schur decomposition, highly transparency and robustness and also faster procedure in comparison with SVD-based methods is obtained. Moreover to enhance transparency and robustness, the watermark encoded by Error Correcting Code is embedded in some blocks of host image, selected by Logistic map. The experimental results confirm the efficiency of the proposed scheme.

IV. PROBLEM FORMULATION

Watermarking is not the only method to protect digital content. Cryptographic encryption and digital signatures have also been studied extensively for their use in secure communication and protection of important information. However, watermarking has several important advantages compared to encryption and digital signatures. First, watermarking incorporates an embedding process, preventing easy separation of the watermark from the content. Digital signatures, on the other hand, are attached to the files as headers, which can be deleted by re-recording files or be changed by format conversion. Encrypted signals, once decrypted, would have no protection against further manipulations. Secondly, watermarks usually undergo the same changes as the original content. It is possible, by examining the changes in watermarks, to detect the locations and the type of manipulations in the original signal.

V. CONCLUSION

Their differences depend on the design philosophy and the specific applications. Information hiding is a general term for a variety of applications which includes not only data embedding, but also keeping information secret. Therefore, the term information hiding often covers both steganography and watermarking. Steganography is the art of concealing information. the majority of the information that involves sound, image and video is stored in digital form. Multimedia in digital form offers many advantages and new potentials to the average user. Likely the most common used potential of digital media is the untroubled copy without degradation of the medium. Another convenience of digital multimedia is the ability of easy modification of its content. The above actions may be permissible, like the legitimate copy of a medical digital image for remote diagnosis purposes, or non permissible, like the illegal copy and distribution of a digital music album.

REFERENCES

[1]. P. Rasti, G. Anbarjafari and H. Demirel, "Colour image watermarking based on wavelet and QR decomposition," 2017 25th Signal Processing and Communications Applications Conference (SIU), Antalya, 2017, pp. 1-4.

[2]. N. N. Hurrah, N. A. Loan, S. A. Parah and J. A. Sheikh, "A transform domain based robust color image watermarking scheme for single and dual attacks," 2017 Fourth International Conference on Image Information Processing (ICIIP), Shimla, India, 2017, pp. 1-5.

[3]. Q. Su, "Novel blind colour image watermarking technique using Hessenberg decomposition," in IET Image Processing, vol. 10, no. 11, pp. 817-829, 11 2016.

[4]. S. Deepa and A. Sandeep, "ROI lossless colored medical image watermarking scheme with secure embedding of patient data," 2016 International Conference on Communication Systems and Networks (ComNet), Thiruvananthapuram, 2016, pp. 103-106.

[5]. A. M. A. Najih, S. A. R. Al-Haddad, A. R. Ramli and S. J. Hashim, "A New Colour Image Watermarking Technique Using Special Domain," 2015 5th International Conference on IT Convergence and Security (ICITCS), Kuala Lumpur, 2015, pp. 1-5.

[6]. R. Mothi and M. Karthikeyan, "Color image watermarking using wavelet packet transform," 2014 IEEE International Conference on Computational Intelligence and Computing Research, Coimbatore, 2014, pp. 1-5.

[7]. F. O. Owalla and E. Mwangi, "A colour image watermarking technique resistant to affine geometric attacks," 2013 Africon, Pointe-Aux-Piments, 2013, pp. 1-5.

[8]. N. Panahi, M. Amirani, S. Behnia and P. Ayubi, "A new colour image watermarking scheme using Cellular Automata Transform and Schur decomposition," 2013 21st Iranian Conference on Electrical Engineering (ICEE), Mashhad, 2013, pp. 1-5.